AF IFW
2132

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Geoffrey S. Strongin, et al

Serial No.: 09/870,890

Filed: May 30, 2001

For: SECURE BOOTING OF A PERSONAL COMPUTER SYSTEM

Examiner: V. Perungavoor

Group Art Unit: 2132

Att'y Docket: 2000.080100

Customer No. 023720

APPEAL BRIEF

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

11/10/05 (Date)

Kathy Danas (Signature)

Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated June 21, 2005. A Notice of Appeal was filed on September 21, 2005 and so this Appeal Brief is believed to be timely filed.

The Commissioner is authorized to deduct the fee for filing this Appeal Brief ($500) from **Advanced Micro Devices, Inc.'s Deposit Account 01-0365/TT4828.**[1]

11/15/2005 EFLORES 00000034 010365 09870890
01 FC:1402 500.00 DA

[1] In the event the monies in that account are insufficient, the Director is authorized to withdraw funds from Williams, Morgan & Amerson, P.C. Deposit Account No. 50-0786/2000.080100.

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 11882, Frame 0867.

II. RELATED APPEALS AND INTERFERENCES

Applicant is not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-24 are pending in the application. Claims 1-24 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Muller *et al.* (U.S. Patent No. 6,256,740).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 9, and 17 set forth establishing a secret between two or more devices in a computer system and securing the secret in each of the two or more devices. Establishing the secret between two or more devices may include transmitting a first GUID from a first device to a master device. Securing the secret in each of the two or more devices may therefore include storing the first GUID in a GUID table in the master device, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

For example, in one embodiment of the present invention, at boot time or during some other trusted set-up, a south bridge 330D and/or a processor 805F or other master device transmits a secret 4095 to each of the devices coupled to the master device capable of storing the secret 4095. Thus, in the illustrated embodiment of Fig. 29A, the USB hub 4015, the biometric device 4020, and the smart card reader 4025 would each store the secret 4095. In other words, during the trusted set-up, the device or devices become known to the master device through an authentication routine, and the master device communicates the secret 4095 to those devices that authenticate properly as a trusted component of the computer subsystem 4000 or some part of the computer system. During data requests or transfers, the master device transmits a random number (or at least a nonce, a number that is used only once) to the device along with the data request. The device may encrypt the data using the random number (or the nonce) and the secret before transmitting the data to the master device. See Patent Application, page 75, ll. 10-23.

As an example of this embodiment, consider the biometric device 4020 of Fig. 29A as a fingerprint scanner 4020. Placing a finger on the fingerprint scanner 4020 may cause the fingerprint scanner 4020 to send an interrupt to the system. The fingerprint scanner 4020 scans the fingerprint of the finger on the fingerprint scanner 4020 to create fingerprint data. The system notifies the south bridge 330D, which sends the nonce to the fingerprint scanner 4020. The fingerprint scanner 4020 receives the nonce and returns the fingerprint data and the nonce to the south bridge 330D in response to receiving the nonce. The fingerprint scanner 4020 may also encrypt the fingerprint data using the nonce in lieu of sending the fingerprint data in the clear (*i.e.* not encrypted). See Patent Application, page 76, ll. 1-9.

At boot time or during some other trusted set-up, the south bridge 330D and/or the processor 805F or other master device may also read the GUIDs from each device coupled to the

south bridge 330D (*i.e.* the master device) capable of storing or actually storing a GUID 4099. Thus, in the illustrated embodiment of Fig. 29A, the USB hub 4015, the biometric device 4020, the smart card reader 4025, and the keyboard 4019 each have GUIDs 4099B, 4099A, 4099D, and 4099C, respectively. The south bridge 330D stores the GUIDs for each device in the GUID table 4098. In other words, during the trusted set-up, the device or devices become known to the south bridge 330D through an authentication routine, and the devices communicate their respective GUIDs 4099 to the south bridge 330D that authenticates them as a trusted component of the computer subsystem 4000 or some part of the computer system. See Patent Application, page 76, ll. 10-22.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the single rejection present in this case. The following issue is presented on appeal in this case:

(A) Whether claims 1-24 are anticipated by Muller.

VII. ARGUMENT

A. Legal Standards

An anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

B. Claims 1-24 Are Not Anticipated by Muller *et al.*

Muller is concerned with assigning names to numerous storage extents that may be assigned to one or more processors. Muller therefore describes a technique for generating a globally unique identifier (ID) and exporting the globally unique identifier to one or more compute nodes via an interconnect fabric. Muller states that a message including a signature that securely identifies a compute node may be sent before the globally unique identifier is transmitted. The globally unique identifier may be transmitted to the compute node if the signature is authenticated, but if the signature is not authenticated, the globally unique identifier is not transmitted to the compute node. See Muller, col. 41, ll. 41-62 and Figure 14.

However, Muller is completely silent with regard to *securing* the globally unique identifier *after* it has been transmitted to the compute node. In particular, Muller fails to teach or suggest preventing access to the globally unique identifier after it has been transmitted to the compute node. To the contrary, Muller teaches that the globally unique identifier may include information indicating local access rights for the data associated with the globally unique identifier. See Muller, col. 41, ll. 51-53. Muller teaches that the globally unique identifier should be presented as a device point in the compute node, *e.g.*, the globally unique identifier should be visible and available to be accessed by other devices so that the local access rights may be determined. See Muller, col. 41, line 56-col. 42, line 1. Appellants therefore submit that Muller fails to teach or suggest establishing a secret between two or more devices and securing the secret *in* each of the two or more devices, as set forth in independent claims 1, 9, and 17.

For at least the aforementioned reasons, Appellants respectfully submit that the present invention is not anticipated by Muller and request that the Examiner's rejections of claims 1-24 under 35 U.S.C. 102(b) be REVERSED.

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-24 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 1-24, over the prior art of record. The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: 11/10/05

Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

CLAIMS APPENDIX

1. A method of booting a computer system, the method comprising:

establishing a secret between two or more devices; and

securing the secret in each of the two or more devices.

2. The method of claim 1, wherein establishing the secret between two or more devices comprises providing a first GUID from a first device to a master device; and

wherein securing the secret in each of the two or more devices comprises storing the first GUID in a GUID table in the master device, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

3. The method of claim 2, further comprising:

the first device setting an introduced bit in response to providing the first GUID from the first device to the master device.

4. The method of claim 2, wherein establishing the secret between two or more devices further comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices further comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

5. The method of claim 1, wherein establishing the secret between two or more devices comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

6. The method of claim 5, further comprising:

the first device setting an introduced bit in response to providing the system GUID from the master device to at least the first device.

7. The method of claim 1, wherein establishing the secret between two or more devices comprises a master device providing a value to a first device as a first GUID; and wherein securing the secret in each of the two or more devices comprises the first device storing the first GUID in a storage location, the master device storing the first GUID in a GUID table, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

8. The method of claim 7, wherein establishing the secret between two or more devices further comprises the master device obtaining a random number and the master device providing the random number to the first device as the first GUID.

9. A method for booting a computer system, the method comprising:

step for establishing a secret between two or more devices; and

step for securing the secret in each of the two or more devices.

10. The method of claim 9, wherein the step for establishing the secret between two or more devices comprises step for providing a first GUID from a first device to a master device; and wherein the step for securing the secret in each of the two or more devices comprises step for storing the first GUID in a GUID table in the master device, step for preventing access to the first GUID in the first device, and step for preventing access to the GUID table in the master device.

11. The method of claim 10, further comprising:

step for the first device setting an introduced bit in response to the step for providing the first GUID from the first device to the master device.

12. The method of claim 10, wherein the step for establishing the secret between two or more devices further comprises step for providing a system GUID from a master device to at least a first device; and wherein the step for securing the secret in each of the two or more devices further comprises step for storing the system GUID in a storage location in at least the first device, step for preventing access to the system GUID in the storage location in at least the first device, and step for preventing access to the system GUID in the master device.

13. The method of claim 9, wherein the step for establishing the secret between two or more devices comprises step for providing a system GUID from a master device to at least a first

device; and wherein the step for securing the secret in each of the two or more devices comprises step for storing the system GUID in a storage location in at least the first device, step for preventing access to the system GUID in the storage location in at least the first device, and step for preventing access to the system GUID in the master device.

14. The method of claim 13, further comprising:

step for the first device setting an introduced bit in response to providing the system GUID from the master device to at least the first device.

15. The method of claim 9, wherein the step for establishing the secret between two or more devices comprises step for a master device providing a value to a first device as a first GUID; and wherein the step for securing the secret in each of the two or more devices comprises step for the first device storing the first GUID in a storage location, step for the master device storing the first GUID in a GUID table, step for preventing access to the first GUID in the first device, and step for preventing access to the GUID table in the master device.

16. The method of claim 15, wherein the step for establishing the secret between two or more devices further comprises step for the master device obtaining a random number and step for the master device providing the random number to the first device as the first GUID.

17. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of booting the computer system, the method comprising:

establishing a secret between two or more devices; and

securing the secret in each of the two or more devices.

18. The computer readable program storage device of claim 17, wherein establishing the secret between two or more devices comprises providing a first GUID from a first device to a master device; and

wherein securing the secret in each of the two or more devices comprises storing the first GUID in a GUID table in the master device, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

19. The computer readable program storage device of claim 18, the method further comprising:

the first device setting an introduced bit in response to providing the first GUID from the first device to the master device.

20. The computer readable program storage device of claim 18, wherein establishing the secret between two or more devices further comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices further comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

21. The computer readable program storage device of claim 17, wherein establishing the secret between two or more devices comprises providing a system GUID from a master device to at least a first device; and wherein securing the secret in each of the two or more devices comprises storing the system GUID in a storage location in at least the first device, preventing access to the system GUID in the storage location in at least the first device, and preventing access to the system GUID in the master device.

22. The computer readable program storage device of claim 21, the method further comprising:

the first device setting an introduced bit in response to providing the system GUID from the master device to at least the first device.

23. The computer readable program storage device of claim 17, wherein establishing the secret between two or more devices comprises a master device providing a value to a first device as a first GUID; and wherein securing the secret in each of the two or more devices comprises the first device storing the first GUID in a storage location, the master device storing the first GUID in a GUID table, preventing access to the first GUID in the first device, and preventing access to the GUID table in the master device.

24. The computer readable program storage device of claim 23, wherein establishing the secret between two or more devices further comprises the master device obtaining a random number and the master device providing the random number to the first device as the first GUID.